QUINN EMANUEL URQUHART & SULLIVAN, LLP
John Neukom (Bar No. 275887)
johnneukom@quinnemanuel.com
Andrew M. Holmes (Bar No. 260475)
drewholmes@quinnemanuel.com
Alicia Veglia (Bar No. 291070)
aliciaveglia@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, California 94111-4788
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Attorneys for Fortinet, Inc.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

FORTINET, INC., Plaintiff, vs. FIREEYE, INC., Defendant.	CASE NO. 5:13-cv-02496-EJD **JURY TRIAL DEMANDED**

SECOND AMENDED COMPLAINT

Plaintiff Fortinet, Inc. ("Fortinet") for its Second Amended Complaint against Defendant FireEye, Inc. ("FireEye") alleges upon knowledge as to itself and its own actions and upon information and belief as to all other matters as follows:

Events Since Fortinet's First Amended Complaint

Since the filing of this lawsuit two years ago, where Fortinet alleged patent infringement and trade secret misappropriation by FireEye, FireEye has continued its pattern of conduct misappropriating Fortinet's intellectual property. Partially as a result of this, FireEye has grown substantially. As one example, FireEye's revenue for 2013 was $161.6 million, an increase in 94 percent from 2012.[1] As another example, FireEye's customers grew from 927 to 2,078 between 2012 and 2013.[2] As of the date of the filing of this Second Amended Complaint, FireEye has a market cap of $3.99 billion.[3]

FireEye's strategy of delay has resulted in the delay of resolution of the merits of this litigation for two years, during which FireEye's conduct has continued unabated. Fortinet files this second amended complaint not only to recover past damages, but to recover these continued damages, which have been created by FireEye's continued misappropriation of Fortinet's intellectual property rights.

INTRODUCTION

1. Fortinet brings this action against FireEye to seek remedies for FireEye's infringement of U.S. Patent Nos. 8,056,135 ("the '135 patent"), 8,204,933 ("the '933 patent"), 7,580,974 ("the '974 patent"), 7,979,543 ("the '543 patent"), 8,051,483 ("the '483 patent"), and 8,276,205 ("the '205 patent") (collectively, the "Asserted Patents").

2. Fortinet also brings this action against FireEye to seek remedies for FireEye's (i) deliberate and willful misappropriation of Fortinet trade secrets, and (ii) intentional interference with one or more Fortinet contracts, all of which caused and continue to cause significant harm to Fortinet.

PARTIES

3. Fortinet is a Delaware corporation with a principal place of business at 1090 Kifer Road, Sunnyvale, California 94086. Since 2000, Fortinet has been a leading provider of network security appliances, appliances and services, and a market leader in unified threat management systems. Fortinet currently employs 1800 individuals worldwide to serve its more than 125,000 customers around the globe.

[1] *See* FireEye Annual Report 2013, available at http://files.shareholder.com/downloads/AMDA-254Q5F/3548616138x0x747474/14d5902e-e763-4293-8565-12d5cc1c3ca9/FireEye_2014_Proxy_Statement_2013_Annual_Report_on_Form_10-K.PDF (last accessed Oct. 15, 2014).

[2] *See id*.

[3] *See* http://finance.yahoo.com/q?s=FEYE (last accessed Oct. 15, 2014).

4. On information and belief, FireEye is a corporation organized under the laws of Delaware with a principal place of business at 1440 McCarthy Blvd., Milpitas, California 95035.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a) because this lawsuit is a civil action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 101 *et seq*. This Court has supplemental jurisdiction over Fortinet's related state law claims pursuant to 28 U.S.C. § 1367.

6. This Court has personal jurisdiction over FireEye. On information and belief, FireEye has significant contacts with this forum and conducts and has conducted business within this forum and within this District. On information and belief, FireEye makes infringing products that are and have been offered for sale, sold, purchased, and used in this District. On information and belief, FireEye directly and/or through its sales and distribution network—including partners, subsidiaries, distributors, retailers, third party administrators, and/or others—places infringing products within the stream of commerce with the knowledge and/or understanding that such infringing products will be sold and used in this District. On information and belief, FireEye is a Delaware corporate entity, and also has a registered agent in this District for the purposes of accepting service of process. FireEye thus lacks any objection to this Court's personal jurisdiction.

7. Venue is proper in this District under 28 U.S.C. §§ 1391(b)-(c) and 1400(b) because FireEye resides in this District and because a substantial part of the events or omissions giving rise to these claims occurred in this District, including FireEye's acts of patent infringement.

FACTUAL BACKGROUND

8. Founded in 2000, Fortinet is a leader and worldwide provider of innovative network security appliances and unified threat management solutions. In just over a decade, Fortinet has earned the trust of thousands of companies that use Fortinet's market-leading security solutions to protect their critical networks, databases, and applications. Fortinet's worldwide

customers represent all verticals, including leading telecommunication carriers and multi-national enterprises.

9. Fortinet is a pioneer in the fields of network security and unified threat management and has expended substantial resources researching and developing its technology. This research and development has led to numerous innovative products in the network security market. The United States Patent and Trademark Office has recognized Fortinet's achievements by awarding numerous patents to Fortinet and its inventors as a result of these innovations. In addition to these Fortinet patents, Fortinet also owns other patents in the network security field that it has acquired over the past decade.

10. On information and belief, since around 2004, Fortinet has competed with FireEye in the network security industry.

FireEye's Corporate Raiding of Fortinet

11. Since entering the network security market, FireEye has sought to acquire business and engineering expertise in the industry. But instead of relying on its own ingenuity and lawful business practices, FireEye's growth strategy has included competitor raids and trade secret misappropriation.

12. Since 2008, FireEye has hired at least eleven Fortinet employees from Fortinet's key divisions, including Fortinet product managers, marketing experts, security and systems engineers, account managers, and senior sales managers (hereinafter, the "Former Fortinet Employees"). Nine of these Former Fortinet Employees—including Fortinet's former Vice President of Product Management and Product Marketing—were hired in the past two and a half years.

Fortinet's Trade Secrets

13. Throughout the Former Fortinet Employees' employment at Fortinet, they received, acquired intimate knowledge of, and were otherwise privy to highly sensitive and valuable trade secret information about Fortinet customers (lists, contacts, sales data, trends, preferences, financials, leads), partners (lists, contacts, financials, distribution channels), Fortinet products (business plans, marketing, sales, pricing, tests, competitive intelligence), unique Fortinet

employment information (proprietary compilations of data with salary and compensation package information), among other information (collectively, the “Fortinet Trade Secrets”). And when they left for FireEye, the Former Fortinet Employees illegally took these valuable Fortinet Trade Secrets with them for the benefit of FireEye.

14. At all relevant times, Fortinet took reasonable and necessary precautions to guard the secrecy and safety of the Fortinet Trade Secrets. Fortinet protects its facilities, servers, computers, networks, databases, and communications systems using a variety of physical and electronic security systems, such as access cards, password protection systems, firewalls, and encrypted communications technology. Fortinet also requires its employees—including the Former Fortinet Employees—to read, acknowledge, and sign an employment agreement and/or a proprietary information and inventions agreement swearing them to secrecy and loyalty.

15. The employment agreement explicitly informs all employees that Fortinet’s “proprietary information is extremely important” and that employment is “expressly subject to your executing a Proprietary Information and Inventions Agreement.” The Former Fortinet Employees thus executed a Proprietary Information and Inventions Agreement and agreed that: “At all times during the term of my employment and thereafter, I will hold in strictest confidence and will not disclose, use, lecture upon or publish any of the Company’s Proprietary Information,” which includes, among other information, “information regarding plans for research, development, new products, marketing and selling, business plans, budgets and unpublished financial statements, licenses, prices and costs, suppliers and customers; and information regarding the skills and compensation of other employees of the Company.”

16. The Former Fortinet Employees also agreed “that for the period of my employment by the Company and for one (1) year after the date of termination of my employment by the Company, I will not (i) induce any employee of the Company to leave the employ of the Company or (ii) solicit business of any client or customer of the Company (other than on behalf of the Company).”

17. On information and belief, prior to hiring the Former Fortinet Employees, FireEye knew or had reason to know of the Former Fortinet Employees’ contractual obligations

regarding confidential and valuable Fortinet Trade Secrets; FireEye decided to and did interfere with those contracts by causing or substantially causing their breach.

FireEye's Theft of Fortinet Trade Secrets

18. Despite their contractual obligations to Fortinet, the Former Fortinet Employees worked with FireEye, a Fortinet competitor, while they were employed by Fortinet and after they were employed by Fortinet, and failed to disclose that work to Fortinet. While the Former Fortinet Employees were employed by Fortinet and thereafter, the Former Fortinet Employees misappropriated and misused Fortinet property and Fortinet resources for the benefit of themselves and FireEye, and thereby breached their contractual obligations with Fortinet and violated state law trade secret protections.

19. On information and belief, FireEye willfully engaged in a systematic hiring spree of Fortinet employees in order to illegally acquire and improperly enrich itself from the Fortinet Trade Secrets. FireEye since has used and benefited from the Fortinet Trade Secrets without permission from or compensation to Fortinet.

The Law Firm Account

20. For example, one Former Fortinet Employee ("Employee 1") signed his engagement letter with FireEye on a Monday in August 2012, unbeknownst to Fortinet. Two days later, on Wednesday, and while still employed at Fortinet, Employee 1 received internal confidential Fortinet emails regarding a significant account with a large international law firm ("Law Firm"). As is common, the Law Firm was comparing two security providers, Fortinet and FireEye. Employee 1—just days after signing the FireEye engagement letter—was copied on and was actively engaged in preparing a detailed comparison of Fortinet's and FireEye's offerings in response. That same day, Employee 1 surreptitiously forwarded relevant emails related to the Law Firm account and containing and reflecting Fortinet Trade Secrets from his Fortinet email account to his personal email account. On information and belief, Employee 1 stole these Fortinet Trade Secrets in order to compete with Fortinet for at least the Law Firm account, among potentially other sales to Fortinet customers.

21. On information and belief, neither Employee 1 nor FireEye disclosed any of this information to Fortinet.

22. On information and belief, at all times FireEye knew or had reason to know that Fortinet Trade Secrets were obtained from Fortinet by Employee 1 by these improper means. On information and belief, FireEye has used and disclosed those Fortinet Trade Secrets stolen by Employee 1 without Fortinet's consent and without regard to Fortinet's rights, and without compensation, permission, or licenses for the benefit of itself and others. FireEye's conduct was, is, and remains willful and wanton, and was taken with blatant disregard for Fortinet's valid and enforceable rights.

23. FireEye also knowingly and intentionally induced, or attempted to induce, at least Employee 1 to violate his or her contractual obligations to Fortinet by stealing Fortinet Trade Secrets related to at least the Law Firm account.

24. Further, FireEye and Employee 1 deliberately intended to disrupt the business relationship between Fortinet and the Law Firm by stealing Fortinet Trade Secrets by and through forwarding Fortinet emails to a personal email account immediately before leaving Fortinet for FireEye. FireEye and Employee 1 were aware of Fortinet's relationship and/or potential relationship with the Law Firm yet stole Fortinet Trade Secrets related to the Law Firm for the use of FireEye, and thus willfully and intentionally interfered with that potential economic advantage to Fortinet's detriment.

International Distributor

25. Fortinet has a significant relationship with a large, international distributor and reseller of network security appliances (the "Distributor"). On information and belief, a Former Fortinet Employee ("Employee 2") was, while employed at Fortinet, a primary Fortinet contact and liaison with the Distributor for sales to Mexico and Latin America.

26. Distributors and resellers like the Distributor are critical to Fortinet's sales channel, as they provide Fortinet with access to new markets, territories, and customer bases, and typically provide high quality service and support. Trusted and well-respected distributors and resellers are valuable to companies like Fortinet and FireEye.

27. Fortinet's internal list of distributors and resellers—and the history and terms of those relationships—are protected, confidential, and extremely valuable to Fortinet.

28. Employee 2's last day at Fortinet was a Friday in August 2012. But shortly thereafter—that same month—Employee 2 began contacting and soliciting the Distributor on behalf of FireEye using Fortinet Trade Secrets. Employee 2 unlawfully attempted both to forge a new relationship with the Distributor for FireEye based on Fortinet Trade Secrets and to disrupt Fortinet's relationship with the Distributor.

29. On information and belief, at all times FireEye knew or had reason to know that Fortinet Trade Secrets were obtained from Fortinet by Employee 2 by improper means. On information and belief, FireEye has used and disclosed those Fortinet Trade Secrets without Fortinet's consent and without regard to Fortinet's rights, and without compensation, permission, or licenses for the benefit of itself and others. FireEye's conduct was, is, and remains willful and wanton, and was taken with blatant disregard for Fortinet's valid and enforceable rights.

30. FireEye also knowingly and intentionally induced, or attempted to induce, at least Employee 2 to violate his or her contractual obligations to Fortinet by stealing Fortinet Trade Secrets related to the Distributor.

31. Further, FireEye and Employee 2 deliberately intended to disrupt the business relationship between Fortinet and the Distributor by stealing Fortinet Trade Secrets in the form of distributor lists and the terms of history of Fortinet's relationship with the Distributor. FireEye and Employee 2 were aware of Fortinet's relationship and/or potential relationship with the Distributor yet stole Fortinet Trade Secrets related to the Distributor for use against Fortinet, and thus willfully and intentionally interfered with that potential economic advantage to Fortinet's detriment.

Fortinet's Salesforce Database

32. Fortinet maintains many Fortinet Trade Secrets on a confidential and secure data repository hosted by Salesforce.com ("Salesforce Database"). The Salesforce Database contains unique, proprietary Fortinet information considered to be the "crown jewels" of Fortinet's sales team. The Salesforce Database maintains information such as (i) lists of all the

Fortinet customer accounts; (ii) billing addresses, shipping addresses, contact information, emails, telephone numbers, contracts, and contact history; (iii) specific customer, distributor, and partner contact information including titles, telephone numbers, email addresses, "if primary" contact, and other certification information; (iv) an "opportunities" page with details about what various account(s) are looking to buy, product lists, sales stage history, and leads (new, current, or future customers); (v) "special pricing requests" which shows Fortinet products and how much of a discount may have been given, who the distributor was, and how much margin the distributor made, among other information; and (vi) forecasts, dashboards, and reports, through which Fortinet sales representatives or managers are able to view forecasts and run sales reports.

33. To access the Salesforce Database, a Fortinet employee first must be pre-approved and granted access by a Fortinet system administrator—at least one such administrator is one of the Fortinet employees raided by FireEye in 2012. This includes having a personal account created with a unique user name and private password. Accounts to Fortinet's Salesforce Database are limited and controlled by Fortinet—only employees who have a "need to know" are given access due to the highly sensitive, valuable Fortinet information contained in the database.

34. Knowing that much of Fortinet's most sensitive, valuable sales information resided in the Salesforce Database, in the days and weeks leading up to their departure from Fortinet to FireEye, numerous Former Fortinet Employees accessed the Salesforce Database at higher-than-normal frequencies in order to steal Fortinet Trade Secrets related to Fortinet sales, leads, customers (current and future), distributors, pricing, and other confidential sales information. As their departure dates neared, Former Fortinet Employees who would login to the Salesforce Database only occasionally during the normal course of their employment *(e.g.*, once or twice a month) began secretly logging into the database with urgency. In fact, two Former Fortinet Employees logged into the Salesforce Database on their last day at Fortinet and one Former Fortinet Employee illegally logged in two days *after* leaving Fortinet.

35. On information and belief, the Former Fortinet Employees accessed the Salesforce Database during their final days at Fortinet with the intent to steal and did steal Fortinet Trade Secrets for, or on behalf of, FireEye and for the benefit of FireEye.

36. On information and belief, at all times FireEye knew or had reason to know that Fortinet Trade Secrets were obtained from Fortinet by Former Fortinet Employees with access to the Salesforce Database by improper means. On information and belief, FireEye has used and disclosed those Fortinet Trade Secrets without Fortinet's consent and without regard to Fortinet's rights, and without compensation, permission, or licenses for the benefit of itself and others. FireEye's conduct was, is, and remains willful and wanton, and was taken with blatant disregard for Fortinet's valid and enforceable rights.

37. FireEye also knowingly and intentionally induced, or attempted to induce, the Former Fortinet Employees to violate their contractual obligations to Fortinet by stealing Fortinet Trade Secrets from the Salesforce Database.

38. By and through their theft of Fortinet Trade Secrets from Fortinet's Salesforce Database, FireEye and the Former Fortinet Employees deliberately intended to disrupt and did disrupt the business relationships between Fortinet and its customers and distributors. FireEye and the Former Fortinet Employees were aware of Fortinet's relationships and/or potential relationships with the customers and distributors listed in the Salesforce Database, yet willfully and intentionally interfered with those potential economic advantages to Fortinet's detriment by unlawfully stealing information about them to use against Fortinet in sales competitions. On information and belief, FireEye has in fact relied upon confidential information, including Fortinet Trade Secrets, stored in the Salesforce Database, in furthering FireEye's business interests.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 8,056,135

39. Fortinet incorporates by reference Paragraphs 1 through 38 as if set forth here in full.

40. Fortinet owns all right, title, and interest in and to the '135 patent, titled "Systems and Methods for Updating Content Detection Devices and Systems." The USPTO duly and legally issued the '135 patent on November 8, 2011. A true and correct copy of the '135 patent is attached to this Second Amended Complaint as Exhibit A.

41. By virtue of its ownership of the ‘135 patent, Fortinet maintains all rights to enforce the ‘135 patent.

42. On information and belief, FireEye has directly infringed, actively induced the infringement of, and/or contributorily infringed one or more claims of the ‘135 patent, including but not limited to Claim 1, in violation of 35 U.S.C. § 271 by (a) making, using, selling, offering for sale, and/or importing into the United States and this District products and services including but not limited to the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated (hereafter collectively referred to as “FireEye Malware Protection Cloud instrumentality”) ; and/or (b) actively inducing others to make, use, sell, offer for sale, and/or import into the United States and this District products and services including but not limited to the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated.

43. FireEye indirectly infringes the ‘135 patent by knowingly and intentionally inducing the infringement of the ‘135 patent by its customers and end users of the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated. On information and belief, FireEye’s current Vice President of Product Management—Fortinet’s former Vice President, Product Management and Product Marketing—has intimate knowledge of Fortinet’s patent portfolio including but not limited to the ‘135 patent. On information and belief, FireEye has intentionally hired other employees from Fortinet; those employees also have awareness of Fortinet’s patent portfolio given the prominent discussion(s) of Fortinet’s patents and intellectual property rights with its employees. And, at a minimum, since at least the filing of the Complaint, FireEye has had knowledge of the ‘135 patent and by continuing the actions described above has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the ‘135 patent.

44. On information and belief FireEye was, and continues to be, aware of the third party’s infringing conduct for the ‘135 patent, including but not limited to FireEye’s

customers and end users use of the FireEye Malware Protection Cloud instrumentality in an infringing manner. On information and belief, FireEye had, and continues to have, the specific intent to cause a third party to infringe the ‘135 patent by virtue of its sales, licenses, partnerships, product demonstrations, partner training, customer support, publishing of product information and documentation and other forms of encouragement of use of the FireEye Malware Protection Cloud instrumentality in an infringing manner. As one example, FireEye's website includes an "InfoCenter"[4] describing the FireEye Malware Protection Cloud instrumentality in white papers, product reports, customer testimonials, case studies, videos, webcasts, webinars, blog postings, product information and other documentation, which encourages third parties to use the FireEye Malware Protection Cloud instrumentality in an infringing manner. Such customer testimonials include specific examples of customers who use the FireEye Malware Protection Cloud instrumentality, such as the University of California at Berkeley[5]; the City of Miramar[6]; Kelsey-Seybold Clinic[7]; D-Wave Systems[8]; and a number of other customers who FireEye does not disclose by name. As another example, FireEye provides Customer Support Services, including but not limited to "[a]nnual on-site review of service and product performance and on-site technical assistance" for third parties, which encourages third parties to use the FireEye Malware Protection Cloud instrumentality in an infringing manner.[9] On information and belief, FireEye had, and continues to have, the specific intent to cause FireEye's customers and end users to infringe the ‘135 patent based on these actions.

[4] *See* http://www.fireeye.com/info-center/ (last accessed Oct. 15, 2014).

[5] *See* http://www.fireeye.com/resources/pdfs/FireEye_HigherEduUCB_casestudy.pdf (last accessed Oct. 15, 2014).

[6] *See* http://www.fireeye.com/resources/pdfs/fireeye-city-of-miramar-cs.pdf (last accessed Oct. 15, 2014).

[7] *See* http://www.fireeye.com/resources/pdfs/fireeye-kelsey-seybold-clinic.pdf (last accessed Oct. 15, 2014).

[8] *See* http://www.fireeye.com/resources/pdfs/fireeye-cs-dwave-systems.pdf (last accessed Oct. 15, 2014).

[9] *See* http://www.fireeye.com/support/support-programs.html (last accessed Oct. 15, 2014).

45. FireEye also contributes to the infringement of the ‘135 patent because, as described above, FireEye is aware of the ‘135 patent and that the FireEye Malware Protection Cloud instrumentality is made for use in infringing the ‘135 patent. As one example, the FireEye Malware Protection Cloud instrumentality, which, for example, can dynamically generate real-time malware intelligence and share this intelligence through the cloud[10], is made for use in updating a content detection module, as described in the ‘135 patent. The FireEye Malware Protection Cloud instrumentality is not a staple article of commerce suitable for substantial non-infringing uses. When customers and end users operate the FireEye Malware Protection Cloud instrumentality for its intended purpose, the FireEye Malware Protection Cloud instrumentality infringes the ‘135 patent. As one example, when customers use the FireEye Malware Protection Cloud instrumentality to “stop[] Web-based attacks,”[11] the FireEye Malware Protection Cloud instrumentality will update a content detection module, as described in the ‘135 patent. It thus has no substantial non-infringing uses and is material to the ‘135 patent. Additionally, the FireEye Malware Protection Cloud instrumentality was especially designed, made, or adapted for use in a manner which infringes the ‘135 patent. On information and belief, FireEye was, and continues, to be aware of these facts and therefore contributes to the infringement of the ‘135 patent. At a minimum, since the filing of the First Amended Complaint, FireEye has knowledge that its customers’ and end users’ use of the FireEye Malware Protection Cloud instrumentality infringes the ‘135 patent.

46. On information and belief, FireEye’s infringement of the ‘135 patent is willful and deliberate, and justifies an increase in damages of up to three times in accordance with 35 U.S.C. § 284. On information and belief, the Vice President and Former Fortinet Employees informed or constructively made FireEye aware of the ‘135 patent. With the knowledge acquired from the Vice President and Former Fortinet Employees, FireEye sold and continues to sell the

[10] *See* http://www.fireeye.com/resources/pdfs/fireeye-web-malware-protection.pdf (last accessed Oct. 15, 2014).

[11] *See id*.

infringing FireEye Malware Protection Cloud instrumentality, despite an objectively high likelihood that its actions constituted infringement of the ‘135 patent. As an example, FireEye has sold the FireEye Malware Protection Cloud instrumentality to customers featured in its customer testimonials, such as the University of California at Berkeley[12]; the City of Miramar[13]; Kelsey-Seybold Clinic[14]; D-Wave Systems[15]; and a number of other customers who FireEye does not disclose by name. As discussed above, FireEye's actions are known to cause infringement of the ‘135 patent, and therefore are willful and deliberate. FireEye's actions in continuing to sell or provide support for the infringing FireEye Malware Protection Cloud instrumentality after becoming aware of the ‘135 patent are objectively reckless.

47. At a minimum, FireEye became aware of the ‘135 patent upon the filing of the First Amended Complaint and that it actions cause infringement of the ‘135 patent by selling the infringing FireEye Malware Protection Cloud instrumentality. With this knowledge, FireEye sold and continues to sell the infringing FireEye Malware Protection Cloud instrumentality. FireEye's actions are known to cause infringement of the ‘135 patent, and therefore are willful and deliberate. FireEye's actions in continuing to sell or provide support for the infringing FireEye Malware Protection Cloud instrumentality after becoming aware of the ‘135 patent are objectively reckless.

48. As a direct and proximate result of FireEye's infringement of the ‘135 patent, Fortinet has suffered monetary damages in an amount not yet determined, and will continue to suffer damages in the future unless FireEye's infringing activities are enjoined by this Court.

[12] *See* http://www.fireeye.com/resources/pdfs/FireEye_HigherEduUCB_casestudy.pdf (last accessed Oct. 15, 2014).

[13] *See* http://www.fireeye.com/resources/pdfs/fireeye-city-of-miramar-cs.pdf (last accessed Oct. 15, 2014).

[14] *See* http://www.fireeye.com/resources/pdfs/fireeye-kelsey-seybold-clinic.pdf (last accessed Oct. 15, 2014).

[15] *See* http://www.fireeye.com/resources/pdfs/fireeye-cs-dwave-systems.pdf (last accessed Oct. 15, 2014).

49. Unless a permanent injunction is issued enjoining FireEye and its officers, agents, employees, and persons acting in active concert or participation with them from infringing the ‘135 patent, Fortinet will be greatly and irreparably harmed.

50. On information and belief, FireEye’s infringement of the ‘135 patent is exceptional and entitles Fortinet to attorneys’ fees and costs under 35 U.S.C. § 285.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 8,204,933

51. Fortinet incorporates by reference Paragraphs 1 through 48 as if set forth here in full.

52. Fortinet owns all right, title, and interest in and to the ‘933 patent, titled “Systems and Methods for Content Type Classification.” The USPTO duly and legally issued the ‘933 patent on June 19, 2012. A true and correct copy of the ‘933 patent is attached to this Second Amended Complaint as Exhibit B.

53. By virtue of its ownership of the ‘933 patent, Fortinet maintains all rights to enforce the ‘933 patent.

54. On information and belief, FireEye has directly infringed, actively induced the infringement of, and/or contributorily infringed one or more claims of the ‘933 patent, including but not limited to Claim 1, in violation of 35 U.S.C. § 271 by (a) making, using, selling, offering for sale, and/or importing into the United States and this District products and services including but not limited to the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine are integrated or otherwise incorporated (hereafter collectively the “FireEye Malware Protective Systems and VX Engines instrumentalities ”); and/or (b) actively inducing others to make, use, sell, offer for sale, and/or import into the United States and this District products and services including but not limited to the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine are integrated or otherwise incorporated.

55. FireEye indirectly infringes the ‘933 patent by knowingly and intentionally inducing the infringement of the ‘933 patent by its customers and end users of the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine are integrated or otherwise incorporated. On information and belief, FireEye’s current Vice President of Product Management—Fortinet’s former Vice President, Product Management and Product Marketing—has intimate knowledge of Fortinet’s patent portfolio including but not limited to the ‘933 patent. On information and belief, FireEye has intentionally hired other employees from Fortinet; those employees also have awareness of Fortinet’s patent portfolio given the prominent discussion(s) of Fortinet’s patents and intellectual property rights with its employees. And, at a minimum, since at least the filing of the Complaint, FireEye has had knowledge of the ‘933 patent and by continuing the actions described above has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the ‘933 patent.

56. On information and belief FireEye was, and continues to be, aware of the third party’s infringing conduct of the ‘933 patent, including but not limited to FireEye’s customers and end users use of the FireEye Malware Protective Systems and VX Engines instrumentalities in an infringing manner. On information and belief, FireEye had, and continues to have, the specific intent to cause a third party to infringe the ‘933 patent by virtue of its sales, licenses, partnerships, product demonstrations, partner training, customer support, publishing of product information and documentation and other forms of encouragement of use of the FireEye Malware Protective Systems and VX Engines instrumentalities in an infringing manner. As one example, FireEye’s website includes an “InfoCenter”[16] describing FireEye Malware Protective Systems and VX Engines instrumentalities in white papers, product reports, customer testimonials, case studies, videos, webcasts, webinars, blog postings, product information and other documentation, which encourages third parties to use the FireEye Malware Protective

[16] *See* http://www.fireeye.com/info-center/ (last accessed Oct. 15, 2014).

Systems and VX Engines instrumentalities in an infringing manner. Such customer testimonials include specific examples of customers who use the FireEye Malware Protective Systems and VX Engines instrumentalities, such as the University of California at Berkeley[17]; the City of Miramar[18]; Kelsey-Seybold Clinic[19]; D-Wave Systems[20]; and a number of other customers who FireEye does not disclose by name. As another example, FireEye provides Customer Support Services, including but not limited to "[a]nnual on-site review of service and product performance and on-site technical assistance" for third parties, which encourages third parties to use the FireEye Malware Protective Systems and VX Engines instrumentalities in an infringing manner.[21] On information and belief, FireEye had, and continues to have, the specific intent to cause FireEye's customers and end users to infringe the '933 patent based on these actions.

57. FireEye also contributes to the infringement of the '933 patent because, as described above, FireEye is aware of the '933 patent and that the FireEye Malware Protective Systems and VX Engines instrumentalities are made for use in infringing the '933 patent. As one example, the FireEye Malware Protective Systems and VX Engines instrumentalities, which, for example, can dynamically generate real-time malware intelligence and share this intelligence through the cloud[22], are made for use in determining a type of content, as described in the '933 patent. As another example, the FireEye Malware Protective Systems and VX Engines instrumentalities, which can "detect[] advanced attacks exploiting unknown vulnerabilities" and "report out forensic details of the exploit,"[23] are made for use in determining a type of content, as

[17] *See* http://www.fireeye.com/resources/pdfs/FireEye_HigherEduUCB_casestudy.pdf (last accessed Oct. 15, 2014).

[18] *See* http://www.fireeye.com/resources/pdfs/fireeye-city-of-miramar-cs.pdf (last accessed Oct. 15, 2014).

[19] *See* http://www.fireeye.com/resources/pdfs/fireeye-kelsey-seybold-clinic.pdf (last accessed Oct. 15, 2014).

[20] *See* http://www.fireeye.com/resources/pdfs/fireeye-cs-dwave-systems.pdf (last accessed Oct. 15, 2014).

[21] *See* http://www.fireeye.com/support/support-programs.html (last accessed Oct. 15, 2014).

[22] *See* http://www.fireeye.com/resources/pdfs/fireeye-web-malware-protection.pdf (last accessed Oct. 15, 2014).

[23] *See id*.

described in the ‘933 patent. The FireEye Malware Protective Systems and VX Engines instrumentalities are not a staple article of commerce suitable for substantial non-infringing uses. When customers and end users operate the FireEye Malware Protective Systems and VX Engines instrumentalities for their intended purpose, the FireEye Malware Protective Systems and VX Engines instrumentalities infringe the ‘933 patent. As one example, when customers use the FireEye Malware Protection Systems and VX Engines instrumentalities to “stop[] Web-based attacks,”[24] the FireEye Malware Protective Systems and VX Engines instrumentalities will determine a type of content, as described in the ‘933 patent. FireEye Malware Protective Systems and VX Engines instrumentalities thus have no substantial non-infringing uses and are material to the ‘933 patent. Additionally, the FireEye Malware Protective Systems and VX Engines instrumentalities were especially designed, made, or adapted for use in a manner which infringes the ‘933 patent. On information and belief, FireEye was, and continues to be, aware of these facts and therefore contributes to the infringement of the ‘933 patent. At a minimum, since the filing of the First Amended Complaint, FireEye has knowledge that its customers’ and end users’ use of the FireEye Malware Protective Systems and VX Engines instrumentalities infringe the ‘933 patent.

58. On information and belief, FireEye’s infringement of the ‘933 patent is willful and deliberate, and justifies an increase in damages of up to three times in accordance with 35 U.S.C. § 284. On information and belief, the Vice President and Former Fortinet Employees informed or constructively made FireEye aware of the ‘933 patent. With the knowledge acquired from the Vice President and Former Fortinet Employees, FireEye sold and continues to sell the infringing FireEye Malware Protective Systems and VX Engines instrumentalities, despite an objectively high likelihood that its actions constitute infringement of the ‘933 patent. As an example, FireEye has sold the FireEye Malware Protective Systems and VX Engines instrumentalities to customers featured in its customer testimonials, such as the University of

[24] *See id.*

California at Berkeley[25]; the City of Miramar[26]; Kelsey-Seybold Clinic[27]; D-Wave Systems[28]; and a number of other customers who FireEye does not disclose by name. As discussed above, FireEye's actions are known to cause infringement of the '933 patent, and therefore are willful and deliberate. FireEye's actions in continuing to sell or provide support for the infringing FireEye Malware Protective Systems and VX Engines instrumentalities after becoming aware of the '933 patent are objectively reckless.

59. At a minimum, FireEye became aware of the '933 patent upon the filing of the First Amended Complaint and that it actions cause infringement of the '933 patent by selling the infringing FireEye Malware Protective Systems and VX Engines instrumentalities. With this knowledge, FireEye sold and continues to sell , the infringing FireEye Malware Protective Systems and VX Engines instrumentalities. FireEye's actions are known to cause infringement of the '933 patent, and therefore are willful and deliberate. FireEye's actions in continuing to sell or provide support for the infringing FireEye Malware Protective Systems and VX Engines instrumentalities after becoming aware of the '933 patent are objectively reckless.

60. As a direct and proximate result of FireEye's infringement of the '933 patent, Fortinet has suffered monetary damages in an amount not yet determined, and will continue to suffer damages in the future unless FireEye's infringing activities are enjoined by this Court.

61. Unless a permanent injunction is issued enjoining FireEye and its officers, agents, employees, and persons acting in active concert or participation with them from infringing the '933 patent, Fortinet will be greatly and irreparably harmed.

[25] *See* http://www.fireeye.com/resources/pdfs/FireEye_HigherEduUCB_casestudy.pdf (last accessed Oct. 15, 2014).

[26] *See* http://www.fireeye.com/resources/pdfs/fireeye-city-of-miramar-cs.pdf (last accessed Oct. 15, 2014).

[27] *See* http://www.fireeye.com/resources/pdfs/fireeye-kelsey-seybold-clinic.pdf (last accessed Oct. 15, 2014).

[28] *See* http://www.fireeye.com/resources/pdfs/fireeye-cs-dwave-systems.pdf (last accessed Oct. 15, 2014).

62. On information and belief, FireEye's infringement of the '933 patent is exceptional and entitles Fortinet to attorneys' fees and costs under 35 U.S.C. § 285.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 7,580,974

63. Fortinet incorporates by reference Paragraphs 1 through 58 as if set forth here in full.

64. Fortinet owns all right, title, and interest in and to the '974 patent, titled "Systems and Methods for Content Type Classification." The USPTO duly and legally issued the '974 patent on August 25, 2009. A true and correct copy of the '974 patent is attached to this Second Amended Complaint as Exhibit C.

65. By virtue of its ownership of the '974 patent, Fortinet maintains all rights to enforce the '974 patent.

66. On information and belief, FireEye has directly infringed, actively induced the infringement of, and/or contributorily infringed one or more claims of the '974 patent, including but not limited to Claim 1, in violation of 35 U.S.C. § 271 by (a) making, using, selling, offering for sale, and/or importing into the United States and this District products and services including but not limited to the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine are integrated or otherwise incorporated; and/or (b) actively inducing others to make, use, sell, offer for sale, and/or import into the United States and this District products and services including but not limited to the FireEye Malware Protection System and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine are integrated or otherwise incorporated.

67. FireEye indirectly infringes the '974 patent by knowingly and intentionally inducing the infringement of the '974 patent by its customers and end users of the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Protection System(s) and Virtual Execution (VX)

Engine are integrated or otherwise incorporated. On information and belief, FireEye's current Vice President of Product Management—Fortinet's former Vice President, Product Management and Product Marketing—has intimate knowledge of Fortinet's patent portfolio including but not limited to the '974 patent. On information and belief, FireEye has intentionally hired other employees from Fortinet; those employees also have awareness of Fortinet's patent portfolio given the prominent discussion(s) of Fortinet's patents and intellectual property rights with its employees. And, at a minimum, since at least the filing of the First Amended Complaint, FireEye has had knowledge of the '974 patent and by continuing the actions described above has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the '974 patent.

68. On information and belief FireEye was, and continues to be, aware of the third party's infringing conduct of the '974 patent, including but not limited to FireEye's customers' and end users' use of the FireEye Malware Protective Systems and VX Engines instrumentalities in an infringing manner. On information and belief, FireEye had, and continues to have, the specific intent to cause a third party to infringe the '974 patent by virtue of its sales, licenses, partnerships, product demonstrations, partner training, customer support, publishing of product information and documentation and other forms of encouragement of use of the FireEye Malware Protective Systems and VX Engines instrumentalities in an infringing manner. As one example, FireEye's website includes an "InfoCenter"[29] describing FireEye Malware Protective Systems and VX Engines instrumentalities in white papers, product reports, customer testimonials, case studies, videos, webcasts, webinars, blog postings, product information and other documentation, which encourages third parties to use the FireEye Malware Protective Systems and VX Engines instrumentalities in an infringing manner. Such customer testimonials include specific examples of customers who use the FireEye Malware Protective Systems and VX

[29] *See* http://www.fireeye.com/info-center/ (last accessed Oct. 15, 2014).

Engines instrumentalities, such as the University of California at Berkeley[30]; the City of Miramar[31]; Kelsey-Seybold Clinic[32]; D-Wave Systems[33]; and a number of other customers who FireEye does not disclose by name. As another example, FireEye provides Customer Support Services, including but not limited to "[a]nnual on-site review of service and product performance and on-site technical assistance" for third parties, which encourages third parties to use of the FireEye Malware Protective Systems and VX Engines instrumentalities in an infringing manner.[34] On information and belief, FireEye had, and continues to have, the specific intent to cause FireEye's customers and end users to infringe the '974 patent based on these actions.

69. FireEye also contributes to the infringement of the '974 patent because, as described above, FireEye is aware of the '974 patent and that the FireEye Malware Protective Systems and VX Engines instrumentalities are made for use in infringing the '974 patent. As one example, the FireEye Malware Protective Systems and VX Engines instrumentalities, which, for example, can dynamically generate real-time malware intelligence and share this intelligence through the cloud[35], are made for use in determining a type of content, as described in the '974 patent. As another example, the FireEye Malware Protective Systems and VX Engines instrumentalities, which can "detect[] advanced attacks exploiting unknown vulnerabilities" and "report out forensic details of the exploit,"[36] are made for use in determining a type of content, as described in the '974 patent. The FireEye Malware Protective Systems and VX Engines instrumentalities are not a staple article of commerce suitable for substantial non-infringing uses.

[30] *See* http://www.fireeye.com/resources/pdfs/FireEye_HigherEduUCB_casestudy.pdf (last accessed Oct. 15, 2014).

[31] *See* http://www.fireeye.com/resources/pdfs/fireeye-city-of-miramar-cs.pdf (last accessed Oct. 15, 2014).

[32] *See* http://www.fireeye.com/resources/pdfs/fireeye-kelsey-seybold-clinic.pdf (last accessed Oct. 15, 2014).

[33] *See* http://www.fireeye.com/resources/pdfs/fireeye-cs-dwave-systems.pdf (last accessed Oct. 15, 2014).

[34] *See* http://www.fireeye.com/support/support-programs.html (last accessed Oct. 15, 2014).

[35] *See* http://www.fireeye.com/resources/pdfs/fireeye-web-malware-protection.pdf (last accessed Oct. 15, 2014).

[36] *See id*.

When customers and end users operate the FireEye Malware Protective Systems and VX Engines instrumentalities for their intended purpose, FireEye Malware Protective Systems and VX Engines instrumentalities infringe the ‘974 patent. As one example, when customers use the FireEye Malware Protection Systems and VX Engines instrumentalities to “stop[] Web-based attacks,”[37] the FireEye Malware Protective Systems and VX Engines instrumentalities will determine a type of content, as described in the ‘974 patent. The FireEye Malware Protective Systems and VX Engines instrumentalities thus have no substantial non-infringing uses and are material to the ‘974 patent. Additionally, the FireEye Malware Protective Systems and VX Engines instrumentalities were especially designed, made, or adapted for use in a manner which infringes the ‘974 patent. On information and belief, FireEye was, and continues to be, aware of these facts and therefore contributes to the infringement of the ‘974 patent. At a minimum, since the filing of the First Amended Complaint, FireEye has knowledge that its customers’ and end users’ use of the FireEye Malware Protective Systems and VX Engines instrumentalities infringes the ‘974 patent.

70. On information and belief, FireEye’s infringement of the ‘974 patent is willful and deliberate, and justifies an increase in damages of up to three times in accordance with 35 U.S.C. § 284. On information and belief, the Vice President and Former Fortinet Employees informed or constructively made FireEye aware of the ‘974 patent. With the knowledge acquired from the Vice President and Former Fortinet Employees, FireEye sold and continues to sell the infringing FireEye Malware Protective Systems and VX Engines instrumentalities, despite an objectively high likelihood that its actions constitute infringement of the ‘974 patent. As an example, FireEye has sold the FireEye Malware Protective Systems and VX Engines instrumentalities to customers featured in its customer testimonials, such as the University of California at Berkeley[38]; the City of Miramar[39]; Kelsey-Seybold Clinic[40]; D-Wave Systems[41]; and

[37] *See id.*

[38] *See* http://www.fireeye.com/resources/pdfs/FireEye_HigherEduUCB_casestudy.pdf (last accessed Oct. 15, 2014).

a number of other customers who FireEye does not disclose by name. As discussed above, FireEye's actions are known to cause infringement of the '974 patent, and therefore are willful and deliberate. FireEye's actions in continuing to sell or provide support for the infringing FireEye Malware Protective Systems and VX Engines instrumentalities after becoming aware of the '974 patent are objectively reckless.

71. At a minimum, FireEye became aware of the '974 patent upon the filing of the First Amended Complaint and that it actions cause infringement of the '974 patent by selling the infringing FireEye Malware Protective Systems and VX Engines instrumentalities. With this knowledge, FireEye sold and continues to sell the infringing FireEye Malware Protective Systems and VX Engines instrumentalities. FireEye's actions are known to cause infringement of the '974 patent, and therefore are willful and deliberate. FireEye's actions in continuing to sell or provide support for the infringing FireEye Malware Protective Systems and VX Engines instrumentalities after becoming aware of the '974 patent are objectively reckless.

72. As a direct and proximate result of FireEye's infringement of the '974 patent, Fortinet has suffered monetary damages in an amount not yet determined, and will continue to suffer damages in the future unless FireEye's infringing activities are enjoined by this Court.

73. Unless a permanent injunction is issued enjoining FireEye and its officers, agents, employees, and persons acting in active concert or participation with them from infringing the '974 patent, Fortinet will be greatly and irreparably harmed.

74. On information and belief, FireEye's infringement of the '974 patent is exceptional and entitles Fortinet to attorneys' fees and costs under 35 U.S.C. § 285.

[39] *See* http://www.fireeye.com/resources/pdfs/fireeye-city-of-miramar-cs.pdf (last accessed Oct. 15, 2014).

[40] *See* http://www.fireeye.com/resources/pdfs/fireeye-kelsey-seybold-clinic.pdf (last accessed Oct. 15, 2014).

[41] *See* http://www.fireeye.com/resources/pdfs/fireeye-cs-dwave-systems.pdf (last accessed Oct. 15, 2014).

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 7,979,543

75. Fortinet incorporates by reference Paragraphs 1 through 68 as if set forth here in full.

76. Fortinet owns all right, title, and interest in and to the ‘543 patent, titled “Systems and Methods for Categorizing Network Traffic Content.” The USPTO duly and legally issued the ‘543 patent on July 12, 2011. A true and correct copy of the ‘543 patent is attached to this Second Amended Complaint as Exhibit D.

77. By virtue of its ownership of the ‘543 patent, Fortinet maintains all rights to enforce the ‘543 patent.

78. On information and belief, FireEye has directly infringed, actively induced the infringement of, and/or contributorily infringed one or more claims of the ‘543 patent, including but not limited to Claim 1, in violation of 35 U.S.C. § 271 by (a) making, using, selling, offering for sale, and/or importing into the United States and this District products and services including but not limited to the FireEye Malware Analysis System and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Analysis System and Virtual Execution (VX) Engine are integrated or otherwise incorporated (hereafter collectively the “FireEye Malware Analysis System and VX Engine instrumentalities”); and/or (b) actively inducing others to make, use, sell, offer for sale, and/or import into the United States and this District products and services including but not limited to the FireEye Malware Analysis System and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Analysis System and Virtual Execution (VX) Engine are integrated or otherwise incorporated.

79. FireEye indirectly infringes the ‘543 patent by knowingly and intentionally inducing the infringement of the ‘543 patent by its customers and end users of the FireEye Malware Analysis System and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Analysis System and Virtual Execution (VX) Engine are integrated or otherwise incorporated. On information and belief, FireEye’s current Vice

President of Product Management—Fortinet's former Vice President, Product Management and Product Marketing—has intimate knowledge of Fortinet's patent portfolio including but not limited to the '543 patent. On information and belief, FireEye has intentionally hired other employees from Fortinet; those employees also have awareness of Fortinet's patent portfolio given the prominent discussion(s) of Fortinet's patents and intellectual property rights with its employees. And, at a minimum, since at least the filing of the First Amended Complaint, FireEye has had knowledge of the '543 patent and by continuing the actions described above has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the '543 patent.

80. On information and belief FireEye was, and continues to be, aware of the third party's infringing conduct of the '543 patent, including but not limited to FireEye's customers and end users use of the FireEye Malware Analysis System and VX Engine instrumentalities in an infringing manner. On information and belief, FireEye had, and continues to have, the specific intent to cause a third party to infringe the '543 patent by virtue of its sales, licenses, partnerships, product demonstrations, partner training, customer support, publishing of product information and documentation and other forms of encouragement of use of the FireEye Malware Analysis System and VX Engine instrumentalities in an infringing manner. As one example, FireEye's website includes an "InfoCenter"[42] describing FireEye Malware Analysis System and VX Engine instrumentalities in white papers, product reports, customer testimonials, case studies, videos, webcasts, webinars, blog postings, product information and other documentation, which encourages third parties to use the FireEye Malware Analysis System and VX Engine instrumentalities in an infringing manner. Such customer testimonials include specific examples of customers who use the FireEye Malware Analysis System and VX Engine instrumentalities, such as the University of California at Berkeley[43] and a number of other

[42] *See* http://www.fireeye.com/info-center/ (last accessed Oct. 15, 2014).

[43] *See* http://www.fireeye.com/resources/pdfs/FireEye_HigherEduUCB_casestudy.pdf (last accessed Oct. 15, 2014).

customers who FireEye does not disclose by name. As another example, FireEye provides Customer Support Services, including but not limited to "[a]nnual on-site review of service and product performance and on-site technical assistance" for third parties, which encourages third parties to use the FireEye Malware Analysis System and VX Engine instrumentalities in an infringing manner.[44] On information and belief, FireEye had, and continues to have, the specific intent to cause FireEye's customers and end users to infringe the '543 patent based on these actions.

81. FireEye also contributes to the infringement of the '543 patent because, as described above, FireEye is aware of the '543 patent and that the FireEye Malware Analysis System and VX Engine instrumentalities are made for use in infringing the '543 patent. As one example, the FireEye Malware Analysis System and VX Engine instrumentalities, which, for example, can generate a dynamic and anonymized profile of an attack[45], are made for use in categorizing network traffic content, as described in the '543 patent. The FireEye Malware Analysis System and VX Engine instrumentalities are not a staple article of commerce suitable for substantial non-infringing uses. When customers and end users operate the FireEye Malware Analysis System and VX Engine instrumentalities for their intended purposes, FireEye Malware Analysis System and VX Engine instrumentalities infringe the '543 patent. As one example, when customers use FireEye Malware Analysis System and VX Engine instrumentalities to "safely execute and inspect advanced malware, zero-day, and advanced persistent threat (APT) attacks,"[46] the FireEye Malware Analysis System and VX Engine instrumentalities will determine a type of content, as described in the '543 patent. FireEye Malware Analysis System and VX Engine instrumentalities thus have no substantial non-infringing uses and are material to the '543 patent. Additionally, the FireEye Malware Analysis System and VX Engine instrumentalities were especially designed, made, or adapted for use in a manner which infringes the '543 patent.

[44] *See* http://www.fireeye.com/support/support-programs.html (last accessed Oct. 15, 2014).

[45] *See* http://www.fireeye.com/resources/pdfs/fireeye-malware-analysis.pdf (last accessed Oct. 15, 2014).

[46] *See id*.

On information and belief, FireEye was, and continues to be, aware of these facts and therefore contributes to the infringement of the '543 patent. At a minimum, since the filing of the First Amended Complaint, FireEye has knowledge that its customers' and end users' use of the FireEye Malware Protection Cloud instrumentality infringes the '543 patent.

82. On information and belief, FireEye's infringement of the '543 patent is willful and deliberate, and justifies an increase in damages of up to three times in accordance with 35 U.S.C. § 284. On information and belief, the Vice President and Former Fortinet Employees informed or constructively made FireEye aware of the '543 patent. With the knowledge acquired from the Vice President and Former Fortinet Employees, FireEye sold and continues to sell the infringing FireEye Malware Analysis System and VX Engine instrumentalities, despite an objectively high likelihood that its actions constituted infringement of the '543 patent. As an example, FireEye has sold the FireEye Malware Analysis System and VX Engine instrumentalities to customers featured in its customer testimonials, such as the University of California at Berkeley[47] and a number of other customers who FireEye does not disclose by name. As discussed above, FireEye's actions are known to cause infringement of the '543 patent, and therefore are willful and deliberate. FireEye's actions in continuing to sell or provide support for the infringing FireEye Malware Analysis System and VX Engine instrumentalities after becoming aware of the '543 patent are objectively reckless.

83. At a minimum, FireEye became aware of the '543 patent upon the filing of the First Amended Complaint and that it actions cause infringement of the '543 patent by selling the infringing FireEye Malware Analysis System and VX Engine instrumentalities. With this knowledge, FireEye sold and continues to sell , the infringing FireEye Malware Analysis System and VX Engine instrumentalities. FireEye's actions are known to cause infringement of the '543 patent, and therefore are willful and deliberate. FireEye's actions in continuing to sell or provide

[47] *See* http://www.fireeye.com/resources/pdfs/FireEye_HigherEduUCB_casestudy.pdf (last accessed Oct. 15, 2014).

support for the infringing FireEye Malware Analysis System and VX Engine instrumentalities after becoming aware of the '543 patent are objectively reckless.

84. As a direct and proximate result of FireEye's infringement of the '543 patent, Fortinet has suffered monetary damages in an amount not yet determined, and will continue to suffer damages in the future unless FireEye's infringing activities are enjoined by this Court.

85. Unless a permanent injunction is issued enjoining FireEye and its officers, agents, employees, and persons acting in active concert or participation with them from infringing the '543 patent, Fortinet will be greatly and irreparably harmed.

86. On information and belief, FireEye's infringement of the '543 patent is exceptional and entitles Fortinet to attorneys' fees and costs under 35 U.S.C. § 285.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 8,051,483

87. Fortinet incorporates by reference Paragraphs 1 through 78 as if set forth here in full.

88. Fortinet owns all right, title, and interest in and to the '483 patent, titled "Systems and Methods for Updating Content Detection Devices and Systems." The USPTO duly and legally issued the '483 patent on November 1, 2011. A true and correct copy of the '483 patent is attached to this Second Amended Complaint as Exhibit E.

89. By virtue of its ownership of the '483 patent, Fortinet maintains all rights to enforce the '483 patent.

90. On information and belief, FireEye has directly infringed, actively induced the infringement of, and/or contributorily infringed one or more claims of the '483 patent, including but not limited to Claim 1, in violation of 35 U.S.C. § 271 by (a) making, using, selling, offering for sale, and/or importing into the United States and this District products and services including but not limited to the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated; and/or (b) actively inducing others to make, use, sell, offer for sale, and/or import

into the United States and this District products and services including but not limited to the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated.

91. FireEye indirectly infringes the '483 patent by knowingly and intentionally inducing the infringement of the '483 patent by its customers and end users of the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated. On information and belief, FireEye's current Vice President of Product Management—Fortinet's former Vice President, Product Management and Product Marketing—has intimate knowledge of Fortinet's patent portfolio including but not limited to the '483 patent. On information and belief, FireEye has intentionally hired other employees from Fortinet; those employees also have awareness of Fortinet's patent portfolio given the prominent discussion(s) of Fortinet's patents and intellectual property rights with its employees. And, at a minimum, since at least the filing of the First Amended Complaint, FireEye has had knowledge of the '483 patent and by continuing the actions described above has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the '483 patent.

92. On information and belief FireEye was, and continues to be, aware of the third party's infringing conduct of the '483 patent, including but not limited to FireEye's customers and end users use of the FireEye Malware Protection Cloud instrumentality in an infringing manner. On information and belief, FireEye had, and continues to have, the specific intent to cause a third party to infringe the '483 patent by virtue of its sales, licenses, partnerships, product demonstrations, partner training, customer support, publishing of product information and documentation and other forms of encouragement of use of the FireEye Malware Protection Cloud instrumentality in an infringing manner. As one example, FireEye's website includes an "InfoCenter"[48] describing the FireEye Malware Protection Cloud instrumentality in white papers, product reports, customer testimonials, case studies, videos, webcasts, webinars, blog postings,

[48] *See* http://www.fireeye.com/info-center/ (last accessed Oct. 15, 2014).

product information and other documentation, which encourages third parties to use the FireEye Malware Protection Cloud instrumentality in an infringing manner. Such customer testimonials include specific examples of customers who use the FireEye Malware Protection Cloud instrumentality, such as the University of California at Berkeley[49]; the City of Miramar[50]; Kelsey-Seybold Clinic[51]; D-Wave Systems[52]; and a number of other customers who FireEye does not disclose by name. As another example, FireEye provides Customer Support Services, including but not limited to "[a]nnual on-site review of service and product performance and on-site technical assistance" for third parties, which encourages third parties to use the FireEye Malware Protection Cloud instrumentality in an infringing manner.[53] On information and belief, FireEye had, and continues to have, the specific intent to cause FireEye's customers and end users to infringe the '483 patent based on these actions.

93. FireEye also contributes to the infringement of the '483 patent because, as described above, FireEye is aware of the '483 patent and that the FireEye Malware Protection Cloud instrumentality is made for use in infringing the '483 patent. As one example, the FireEye Malware Protection Cloud instrumentality, which, for example, can dynamically generate real-time malware intelligence and share this intelligence through the cloud[54], is made for use in updating a content detection module, as described in the '483 patent. The FireEye Malware Protection Cloud instrumentality is not a staple article of commerce suitable for substantial non-infringing uses. When customers and end users operate the FireEye Malware Protection Cloud instrumentality for its intended purpose, FireEye Malware Protection Cloud instrumentality

[49] *See* http://www.fireeye.com/resources/pdfs/FireEye_HigherEduUCB_casestudy.pdf (last accessed Oct. 15, 2014).

[50] *See* http://www.fireeye.com/resources/pdfs/fireeye-city-of-miramar-cs.pdf (last accessed Oct. 15, 2014).

[51] *See* http://www.fireeye.com/resources/pdfs/fireeye-kelsey-seybold-clinic.pdf (last accessed Oct. 15, 2014).

[52] *See* http://www.fireeye.com/resources/pdfs/fireeye-cs-dwave-systems.pdf (last accessed Oct. 15, 2014).

[53] *See* http://www.fireeye.com/support/support-programs.html (last accessed Oct. 15, 2014).

[54] *See* http://www.fireeye.com/resources/pdfs/fireeye-web-malware-protection.pdf (last accessed Oct. 15, 2014).

infringes the ‘483 patent, despite an objectively high likelihood that its actions constituted infringement of the ‘483 patent. As one example, when customers use the FireEye Malware Protection Cloud instrumentality to “stop[] Web-based attacks,[55]” the FireEye Malware Protection Cloud instrumentality will update a content detection module, as described in the ‘483 patent. It thus has no substantial non-infringing uses and is material to the ‘483 patent. Additionally, the FireEye Malware Protection Cloud instrumentality was especially designed, made, or adapted for use in a manner which infringes the ‘483 patent. On information and belief, FireEye was, and continues to be, aware of these facts and therefore contributes to the infringement of the ‘483 patent. At a minimum, since the filing of the First Amended Complaint, FireEye has knowledge that its customers’ and end users’ use of the FireEye Malware Protection Cloud instrumentality infringes the ‘483 patent.

94. On information and belief, FireEye’s infringement of the ‘483 patent is willful and deliberate, and justifies an increase in damages of up to three times in accordance with 35 U.S.C. § 284. On information and belief, the Vice President and Former Fortinet Employees informed or constructively made FireEye aware of the ‘483 patent. With the knowledge acquired from the Vice President and Former Fortinet Employees, FireEye sold and continues to sell the infringing FireEye Malware Protection Cloud instrumentality. As an example, FireEye has sold the FireEye Malware Protection Cloud instrumentality to customers featured in its customer testimonials, such as the University of California at Berkeley[56]; the City of Miramar[57]; Kelsey-Seybold Clinic[58]; D-Wave Systems[59]; and a number of other customers who FireEye does not disclose by name. As discussed above, FireEye’s actions are known to cause infringement of the

[55] *See id*.

[56] *See* http://www.fireeye.com/resources/pdfs/FireEye_HigherEduUCB_casestudy.pdf (last accessed Oct. 15, 2014).

[57] *See* http://www.fireeye.com/resources/pdfs/fireeye-city-of-miramar-cs.pdf (last accessed Oct. 15, 2014).

[58] *See* http://www.fireeye.com/resources/pdfs/fireeye-kelsey-seybold-clinic.pdf (last accessed Oct. 15, 2014).

[59] *See* http://www.fireeye.com/resources/pdfs/fireeye-cs-dwave-systems.pdf (last accessed Oct. 15, 2014).

‘483 patent, and therefore are willful and deliberate. FireEye’s actions in continuing to sell or provide support for the infringing FireEye Malware Protection Cloud instrumentality after becoming aware of the ‘483 patent are objectively reckless.

95. At a minimum, FireEye became aware of the ‘483 patent upon the filing of the First Amended Complaint and that it actions cause infringement of the ‘483 patent by selling the infringing FireEye Malware Protection Cloud instrumentality. With this knowledge, FireEye sold and continues to sell the infringing FireEye Malware Protection Cloud instrumentality. FireEye’s actions are known to cause infringement of the ‘483 patent, and therefore are willful and deliberate. FireEye’s actions in continuing to sell or provide support for the infringing FireEye Malware Protection Cloud instrumentality after becoming aware of the ‘483 patent are objectively reckless.

96. As a direct and proximate result of FireEye’s infringement of the ‘483 patent, Fortinet has suffered monetary damages in an amount not yet determined, and will continue to suffer damages in the future unless FireEye’s infringing activities are enjoined by this Court.

97. Unless a permanent injunction is issued enjoining FireEye and its officers, agents, employees, and persons acting in active concert or participation with them from infringing the ‘483 patent, Fortinet will be greatly and irreparably harmed.

98. On information and belief, FireEye’s infringement of the ‘483 patent is exceptional and entitles Fortinet to attorneys’ fees and costs under 35 U.S.C. § 285.

COUNT VI
INFRINGEMENT OF U.S. PATENT NO. 8,276,205

99. Fortinet incorporates by reference Paragraphs 1 through 88 as if set forth here in full.

100. Fortinet owns all right, title, and interest in and to the ‘205 patent, titled “Systems and Methods for Updating Content Detection Devices and Systems.” The USPTO duly and legally issued the ‘205 patent on September 25, 2012. A true and correct copy of the ‘205 patent is attached to this Second Amended Complaint as Exhibit F.

101. By virtue of its ownership of the ‘205 patent, Fortinet maintains all rights to enforce the ‘205 patent.

102. On information and belief, FireEye has directly infringed, actively induced the infringement of, and/or contributorily infringed one or more claims of the ‘205 patent, including but not limited to Claim 1, in violation of 35 U.S.C. § 271 by (a) making, using, selling, offering for sale, and/or importing into the United States and this District products and services including but not limited to the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated; and/or (b) actively inducing others to make, use, sell, offer for sale, and/or import into the United States and this District products and services including but not limited to the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated.

103. Since the filing of the First Amended Complaint, FireEye has had knowledge of the ‘205 patent and by continuing the actions described therein has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the ‘205 patent. Accordingly, after the filing of the First Amended Complaint, FireEye has, and continues to, indirectly infringe the ‘205 patent by knowingly and intentionally inducing the infringement of the ‘205 patent by its customers and end users of the FireEye Malware Protection Cloud instrumentality. On information and belief FireEye was, and continues to be, aware of the third party’s infringing conduct of the ‘205 patent, including but not limited to FireEye’s customers and end users use of the FireEye Malware Protection Cloud instrumentality in an infringing manner. On information and belief, FireEye had, and continues to have, the specific intent to cause a third party to infringe the ‘205 patent by virtue of its sales, licenses, partnerships, product demonstrations, partner training, customer support, publishing of product information and documentation and other forms of encouragement of use of the FireEye Malware Protection Cloud instrumentality in an infringing manner. As one example, FireEye’s website includes an

"InfoCenter"[60] describing the FireEye Malware Protection Cloud instrumentality in white papers, product reports, customer testimonials, case studies, videos, webcasts, webinars, blog postings, product information and other documentation, which encourages third parties to use the FireEye Malware Protection Cloud instrumentality in an infringing manner. Such customer testimonials include specific examples of customers who use the FireEye Malware Protection Cloud instrumentality, such as the University of California at Berkeley[61]; the City of Miramar[62]; Kelsey-Seybold Clinic[63]; D-Wave Systems[64]; and a number of other customers who FireEye does not disclose by name. As another example, FireEye provides Customer Support Services, including but not limited to "[a]nnual on-site review of service and product performance and on-site technical assistance" for third parties, which encourages third parties to use the FireEye Malware Protection Cloud instrumentality in an infringing manner.[65] On information and belief, FireEye had, and continues to have, the specific intent to cause FireEye's customers and end users to infringe the '205 patent based on these actions.

104. FireEye also contributes to the infringement of the '205 patent because, as described above, FireEye is aware of the '205 patent since at least the filing of the First Amended Complaint and that the FireEye Malware Protection Cloud instrumentality is made for use in infringing the '205 patent. When customers and end users operate the FireEye Malware Protection Cloud instrumentality for its intended purpose, FireEye Malware Protection Cloud instrumentality infringes the '205 patent. As one example, when customers use the FireEye

[60] *See* http://www.fireeye.com/info-center/ (last accessed Oct. 15, 2014).

[61] *See* http://www.fireeye.com/resources/pdfs/FireEye_HigherEduUCB_casestudy.pdf (last accessed Oct. 15, 2014).

[62] *See* http://www.fireeye.com/resources/pdfs/fireeye-city-of-miramar-cs.pdf (last accessed Oct. 15, 2014).

[63] *See* http://www.fireeye.com/resources/pdfs/fireeye-kelsey-seybold-clinic.pdf (last accessed Oct. 15, 2014).

[64] *See* http://www.fireeye.com/resources/pdfs/fireeye-cs-dwave-systems.pdf (last accessed Oct. 15, 2014).

[65] *See* http://www.fireeye.com/support/support-programs.html (last accessed Oct. 15, 2014).

Malware Protection Cloud instrumentality to "stop[] Web-based attacks,[66]" the FireEye Malware Protection Cloud instrumentality will update a content detection module, as described in the '205 patent. It thus has no substantial for non-infringing uses and is material to the '205 patent. Additionally, the FireEye Malware Protection Cloud instrumentality was especially designed, made, or adapted for use in a manner which infringes the '205 patent. On information and belief, FireEye was, and continues to be, aware of these facts and therefore contributes to the infringement of the '205 patent.

105. As a direct and proximate result of FireEye's infringement of the '205 patent, Fortinet has suffered monetary damages in an amount not yet determined, and will continue to suffer damages in the future unless FireEye's infringing activities are enjoined by this Court.

106. Unless a permanent injunction is issued enjoining FireEye and its officers, agents, employees, and persons acting in active concert or participation with them from infringing the '205 patent, Fortinet will be greatly and irreparably harmed.

107. On information and belief, FireEye's infringement of the '205 patent is exceptional and entitles Fortinet to attorneys' fees and costs under 35 U.S.C. § 285.

COUNT VII
MISAPPROPRIATION OF TRADE SECRETS
(Cal. Civ. Code § 3426 *et seq.*; Del. Code tit. 6, § 2001 *et seq.)*

108. Fortinet incorporates by reference Paragraphs 1 through 98 as if set forth here in full.

109. "Fortinet Trade Secrets" as used herein means (i) customer and potential customer names, contacts, lists, purchasing histories, purchasing preferences, and purchasing forecasts, among other proprietary customer information and intelligence such as the identity of key corporate "decision makers;" (ii) key business partner, distributor, wholesaler, and value-added reseller names, contacts, and lists, including but not limited to key downstream companies in the sales channel; (iii) non-public product, pricing, marketing, and sales information, including

[66] *See id.*

sales histories, trends, forecasts, plans, techniques, methods, processes, product characteristics, product tests, and other proprietary competitive knowledge and intelligence; (iv) non-public, unique human resources information and employee-specific information, including but not limited to confidential Fortinet competitive salary and compensation package information; and (v) other information owned by Fortinet that was stolen by FireEye, former Fortinet employees, and other persons acting for, on behalf of, or at the direction of FireEye that are legally protected as trade secrets.

110. Prior to FireEye's thefts, the Fortinet Trade Secrets gave Fortinet a significant competitive advantage over its existing and would-be competitors, including FireEye. This advantage, at least as to FireEye, was compromised as a result of FireEye's unlawful activities.

111. Fortinet invested substantial resources to develop the Fortinet Trade Secrets. And the Fortinet Trade Secrets derive independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from their disclosure or use.

112. Fortinet made reasonable efforts under the circumstances to maintain the confidentiality of the Fortinet Trade Secrets. Fortinet's efforts included, but are not limited to, (i) having employees and consultants who may have access the Fortinet Trade Secrets sign confidentiality agreements that oblige them not to disclose the Fortinet Trade Secrets or characteristics of the Fortinet Trade Secrets; (ii) limiting the circulation of said materials within Fortinet; (iii) protecting, limiting, and controlling access to Fortinet properties with security cards, and other physical or electronic means; (iv) protecting, limiting, and controlling access to computers with secure log-in identifications and passwords; (v) limiting each employee's access to electronic files to those that the particular employee needs to access *(i.e.*, information segregation); (vi) educating employees on the nature of Fortinet's information that is confidential and proprietary; and (vii) reminding employees on a regular and periodic basis of their obligation to protect and maintain Fortinet's confidential and proprietary information.

113. Fortinet did not consent to the use of any of the Fortinet Trade Secrets by anyone other than authorized Fortinet employees using them for Fortinet’s own business purposes.

114. On information and belief, as discussed above, certain former Fortinet employees entered into an agreement with FireEye whereby they would misappropriate Fortinet Trade Secrets in order to give FireEye an unfair advantage in the network security marketplace.

115. On information and belief, at least the Former Fortinet Employees (now FireEye employees) willfully and intentionally misappropriated Fortinet Trade Secrets by acquiring, disclosing, and/or using Fortinet Trade Secrets for FireEye’s purposes—for example, by selling or attempting to sell certain FireEye products, services, or other offerings that would compete with Fortinet’s—even though such employees owed a duty to Fortinet to maintain the confidentiality of the Fortinet Trade Secrets.

116. FireEye has illegally obtained Fortinet Trade Secrets as set forth above and through other means of which Fortinet presently is unaware.

117. On information and belief, at all times FireEye knew or had reason to know that Fortinet Trade Secrets were obtained from Fortinet by improper means.

118. On information and belief, FireEye has used and disclosed Fortinet Trade Secrets without Fortinet’s consent and without regard to Fortinet’s rights, and without compensation, permission, or licenses for the benefit of themselves and others.

119. FireEye’s conduct was, is, and remains willful and wanton, and was taken with blatant disregard for Fortinet’s valid and enforceable rights.

120. FireEye’s wrongful conduct has caused and, unless enjoined by this Court, will continue in the future to cause irreparable injury to Fortinet. Fortinet has no adequate remedy at law for such wrongs and injuries. Fortinet is therefore entitled to a permanent injunction restraining and enjoining FireEye and its agents, servants, officers, directors, and employees, and all persons acting there under, in concert with, or on their behalf, from further using in any manner Fortinet Trade Secrets.

121. In addition, as a proximate result of FireEye's misconduct, Fortinet has suffered actual damages, and FireEye has been unjustly enriched.

122. FireEye's misappropriation of Fortinet Trade Secrets was willful and malicious; on information and belief, FireEye misappropriated Fortinet's trade secrets with the deliberate intent to injure Fortinet's business and improve its own. Fortinet is therefore entitled to enhanced damages and reasonable attorneys' fees.

COUNT VIII
INTENTIONAL INTERFERENCE WITH CONTRACTUAL RELATIONS

123. Fortinet incorporates by reference Paragraphs 1 through 113 as if set forth here in full.

124. Valid agreements existed between Fortinet and the Former Fortinet Employees whom FireEye induced to steal and/or with whom FireEye was complicit with in stealing Fortinet Trade Secrets and other proprietary and confidential information during and after their Fortinet employment.

125. At all times herein mentioned, FireEye knew that the Former Fortinet Employees had a duty under their employment agreements not to work for or assist any competitor of Fortinet, such as FireEye, and not to disclose confidential or Fortinet Trade Secrets to any competitor of Fortinet including FireEye.

126. Despite such knowledge, FireEye intentionally and without justification solicited, induced, and encouraged the Former Fortinet Employees to breach their contracts with Fortinet. On information and belief, Defendant's intentional acts were designed to induce breach of disruption of the contractual relationship by inducing and encouraging Former Fortinet Employees to provide Fortinet Trade Secrets and other proprietary and confidential information to FireEye and use that information in a manner that causes harm to Fortinet. FireEye additionally induced the Former Fortinet Employees to violate their agreements with Fortinet by stealing Fortinet Trade Secrets and other proprietary and confidential information during and after their Fortinet employment, including but not limited to hiring the Former Fortinet Employees and

encouraging them to disclose Fortinet Trade Secrets and other proprietary and confidential information to FireEye.

127. As a direct and proximate result of FireEye's efforts and inducements, the Former Fortinet Employees breached their contracts with Fortinet and prevented performance thereof

128. As a result of said breaches substantially caused by FireEye, Fortinet has suffered damages and will imminently suffer further damages, including the loss of its competitive position and lost profits, in an amount to be proven at trial.

129. FireEye performed the aforementioned conduct with malice, fraud, and oppression, and in conscious disregard of Fortinet's rights.

130. Accordingly, Fortinet is entitled to recover exemplary damages from FireEye in an amount to be determined at trial.

DEMAND FOR JURY TRIAL

131. Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Fortinet demands a jury trial on all triable issues.

REQUEST FOR RELIEF

WHEREFORE, Fortinet respectfully prays for:

a. A judgment that FireEye has infringed and continues to infringe one or more claims of each of the Asserted Patents;

b. A judgment that FireEye's infringement of the Asserted Patents is willful and deliberate, and therefore that Fortinet is entitled to treble damages under 35 U.S.C. § 284;

c. A permanent injunction enjoining FireEye, its directors, officers, agents, and employees, and those acting in privity or in concert with them, and their partners, subsidiaries, divisions, successors, and assigns, from further acts of infringement, contributory infringement, or inducement of infringement of the Asserted Patents;

d. An award of damages adequate to compensate Fortinet for FireEye's infringement of the Asserted Patents, including all pre-judgment and post-judgment interest, costs, and that the damages so adjudged be increased by the Court pursuant to 35 U.S.C. § 284;

e. A judgment that this is an exceptional case and that Fortinet be awarded attorneys' fees, costs, and expenses incurred in this action;

f. A judgment that Fortinet be awarded damages as a result of FireEye's misappropriation of Fortinet's trade secrets;

g. A judgment that FireEye be ordered to pay exemplary damages due to its willful and malicious misappropriation of Fortinet's trade secrets with deliberate intent to injure Fortinet's business and improve its own;

h. A judgment that Fortinet be awarded damages as a result of FireEye's intentional interference with Fortinet's contracts;

i. A permanent injunction enjoining FireEye, its agents, officers, assigns and others acting in concert with it from further wrong-doing, and to return all Fortinet Trade Secrets and other confidential and proprietary materials;

j. A judgment that Fortinet be awarded pre-judgment and post-judgment interest on any award; and

k. That the Court award Fortinet any other relief as the Court deems just and proper.

DATED: October 15, 2014

Respectfully,

By: */s/ John M. Neukom*

John M. Neukom (SBN 275887)
Andrew M. Holmes (SBN 260475)
Alicia M. Veglia (Bar No. 291070)
QUINN EMANUEL URQUHART &
SULLIVAN, LLP
50 California Street, 22nd Floor
San Francisco, CA 94111
Tel: 415-875-6600
Fax: 415-875-6700
johnneukom@quinnemanuel.com
drewholmes@quinnemanuel.com
aliciaveglia@quinnemanuel.com

Attorneys for Plaintiff FORTINET, INC.